



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/798,079	03/11/2004	Aaron Charles Newman	AS2	5342
7590 08/24/2007				
Peter S. Canelias Law Offices of Peter S. Canelias Suite 2148 420 Lexington Avenue New York, NY 10170		EXAMINER KIM, PAUL		
		ART UNIT PAPER NUMBER 2161		
		MAIL DATE DELIVERY MODE 08/24/2007 PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/798,079

Applicant(s)

NEWMAN ET AL.

Examiner

Paul Kim

Art Unit

2161

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 03 July 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 89-97 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 89-97 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This Office action is responsive to the following communication: Amendment filed on 3 July 2007.
2. Claims 89-97 are pending and present for examination. Claim 89 is in independent form.

Response to Amendment

3. Claims 89-97 have been added.
4. Claims 22-30 have been cancelled.
5. No claims have been added.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. **Claims 89 and 90** are rejected under 35 U.S.C. 102(b) as being anticipated by Bapat et al (U.S. Patent No. 6,038,563, hereinafter referred to as BAPAT), filed on 25 March 1998, and issued on 14 March 2000.

8. **As per independent claim 89**, BAPAT teaches:

A computer readable medium having code to perform a computer implemented method for protecting a database, comprising:

implementing at least two lightweight modules for monitoring traffic on a network, the at least two lightweight modules running at the application layer (See BAPAT, Figures 3-4, 8-10, and 14);

monitoring the database for a set of executable and unauthorized SQL statements {See BAPAT, Abstract, wherein this reads over "[a] user access request to access management information in the database is intercepted, and the access control procedure is invoked when the user access request is a select statement"; and C18:L19-27, wherein this reads over "every user

Art Unit: 2161

query for information from the tables in the DBMS is checked by the SQL engine 286 against the access rights established by the access privileges module");

actuating each SQL statement as a discrete database event {See BAPAT, C18:L24-27, wherein this reads over "[u]ser queries requesting information from tables to which the user does not have access rights are rejected by the SQL engine"};

analyzing the discrete database event for compliance with a pre-defined set of detection rules {See BAPAT, C17:L15-19, wherein this reads over "a Security Alarm log 293 that is separate from the security audit trail 192, where security alarms are generated and stored in the log only when there is a denial of object access"};

executing the SQL statement when the discrete database event is compliant with the predefined set of rules {See BAPAT, C18:L19-27, wherein this reads over "only queries in full compliance with those access rights are processed"; and C28:L31-37, wherein this reads over "[a]ccess is allowed only for the objects to which the user has appropriate access rights"};

recording the SQL statement in a log file residing in the database {See BAPAT, C17:L5-20, wherein this reads over "the security audit trail 182 stores every access request and the corresponding outcome in its entirety"}.

9. **As per dependent claim 90, BAPAT teaches:**

The computer readable medium having code to perform the computer implemented method for protecting the database of Claim 89 wherein the step of analyzing further comprises:

detecting whether the set of executable and unauthorized SQL statements are queries for a protected data item submitted by a first user before permission to access the protected data item is granted {See BAPAT, C18:L19-40, wherein this reads over "every user query for information from the tables in the DBMS is checked by the SQL engine 286 against the access rights established by the access privileges module"};

granting a second user permissions to at least one set of protected data, the grant of permissions including a read permission, a write permission and an execute permission {See BAPAT, C18:L19-40, wherein this reads over "only queries in full compliance with those access rights are processed"};

recording the grant of permissions to a table in the database {See BAPAT, Figure 4}.

10. **Claim 91** are rejected under 35 U.S.C. 103(a) as being unpatentable over BAPAT as applied to claims 89 and 90, and further in view of Shostack et al (U.S. Patent No. 6,298,445, hereinafter referred to as SHOSTACK), filed on 30 April 1998, and issued on 2 October 2001.

11. **As per dependent claim 91, BAPAT, in combination with SHOSTACK, discloses:**

The computer readable medium having code to perform the computer implemented method for protecting the database of Claim 89 wherein the step of analyzing further comprises the step of:

Art Unit: 2161

installing a listener agent as a first lightweight module, the listener agent for receiving a plurality of database events {See BAPAT, C16:L62-66, wherein this reads over "[t]he log server 290 is preferably a software entity or process that runs on the same computer or computer node as the MIS"};

establishing a communication link between the listener agent and the database {See BAPAT, C16:L55-61, wherein this reads over "only the log server 290 (besides the system administrator) has write access to the event log tables"};

using the listener agent to process the plurality of database events {See BAPAT, C16:L31-39, wherein this reads over "a log server 290 whose primary function is to convert event notifications into SQL insert statements for storing event notifications in the event log"};

processing the plurality of database events by detecting whether an executable SQL statement exploits a buffer overflow vulnerability in the database {See SHOSTACK, Table 1, wherein this reads over "Check for known bugs in the servers . . . that are vulnerable to buffer overflow attacks" and "X-windows. Check for open permissions that allow snooping of remote X session, unpatched libraries and executables vulnerable to buffer overflow attacks"};

forwarding the processed database events to a network accessible console {See BAPAT, C16:L40-54, wherein this reads over "each database tables stores a different type of event notification"};

recording the processed database events to a table in the database {See BAPAT, C16:L31-39, wherein this reads over "a log server 290 whose primary function is to convert event notifications into SQL insert statements for storing event notifications in the event log"}.

While BAPAT fails to expressly disclose a method of "processing the plurality of database events by detecting whether an executable SQL statement exploits a buffer overflow vulnerability in the database," SHOSTACK discloses a method of check for buffer overflow vulnerabilities. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by BAPAT by combining it with the invention disclosed by ROWLAND.

One of ordinary skill in the art would have been motivated to do this modification so that suspicious or malicious activity may be detected and prevented accordingly.

12. **Claim 92** is rejected under 35 U.S.C. 103(a) as being unpatentable over BAPAT as applied to claims 89 and 90, and further in view of Reshef et al (U.S. Patent No. 6,321,337, hereinafter referred to as RESHEF), filed on 9 September 1998, and issued on 20 November 2001.

13. **As per dependent claim 92,**

The computer readable medium having code to perform the computer implemented method for protecting the database of Claim 91, wherein the step of processing the plurality of database events is accomplished by detecting whether an executable SQL

Art Unit: 2161

statement includes an operating system call {See RESHEF, C10:L 21-35, wherein this reads over "[a]ny breach of the permitted flow sequences by disorderly operating system calls or looping will be trapped and logged"}.

While BAPAT fails to expressly disclose a method of "detecting an executable statement includes an operating system call," RESHEF discloses a method of checking for operating system calls which result in a breach of permitted flow sequences. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by BAPAT by combining it with the invention disclosed by RESHEF.

One of ordinary skill in the art would have been motivated to do this modification so that suspicious or malicious activity may be detected and prevented accordingly.

14. **Claims 93-97** are rejected under 35 U.S.C. 103(a) as being unpatentable over BAPAT as applied to claims 89 and 90, and further in view of Rowland (U.S. Patent No. 6,405,318, hereinafter referred to as ROWLAND), filed on 12 March 1999, and issued on 11 June 2002.

15. **As per dependent claim 93**, BAPAT, in combination with ROWLAND, discloses:

The computer readable medium having code to perform the computer implemented method for protecting the database of Claim 89 wherein the step of analyzing further comprises the step of:

installing a listener agent as a first lightweight module, the listener agent for receiving a plurality of database events {See BAPAT, C16:L62-66, wherein this reads over "[t]he log server 290 is preferably a software entity or process that runs on the same computer or computer node as the MIS"};

establishing a communication link between the listener agent and the database {See BAPAT, C16:L55-61, wherein this reads over "only the log server 290 (besides the system administrator) has write access to the event log tables"};

using the listener agent to process the plurality of database events {See BAPAT, C16:L31-39, wherein this reads over "a log server 290 whose primary function is to convert event notifications into SQL insert statements for storing event notifications in the event log"};

processing the plurality of database events by detecting whether the executable SQL statement contains an attempt by a user to perform a write operation on a data dictionary without permission {See BAPAT, C6:L4-11, wherein this reads over "[i]f a suspicious directory name is found 68, the control function is notified"};

forwarding the processed database events to a network accessible console {See BAPAT, C16:L40-54, wherein this reads over "each database tables stores a different type of event notification"};

Art Unit: 2161

recording the processed database events to a table in the database {See BAPAT, C16:L31-39, wherein this reads over "a log server 290 whose primary function is to convert event notifications into SQL insert statements for storing event notifications in the event log"}.

While BAPAT fails to expressly disclose a method "wherein said unauthorized activity is interfering with auditing settings," ROWLAND discloses a method wherein "[i]f a suspicious directory name is found 68, the control function is notified 55" {See ROWLAND, C6:L4-11}. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by BAPAT by combining it with the invention disclosed by ROWLAND.

One of ordinary skill in the art would have been motivated to do this modification so that suspicious or malicious activity may be detected and prevented accordingly.

16. **As per dependent claim 94**, BAPAT, in combination with ROWLAND, discloses:

The computer readable medium having code to perform the computer implemented method for protecting the database of Claim 89 wherein the step of analyzing further comprises the step of:

installing a listener agent as a first lightweight module, the listener agent for receiving a plurality of database events {See BAPAT, C16:L62-66, wherein this reads over "[t]he log server 290 is preferably a software entity or process that runs on the same computer or computer node as the MIS"};

establishing a communication link between the listener agent and the database {See BAPAT, C16:L55-61, wherein this reads over "only the log server 290 (besides the system administrator) has write access to the event log tables"};

using the listener agent to process the plurality of database events {See BAPAT, C16:L31-39, wherein this reads over "a log server 290 whose primary function is to convert event notifications into SQL insert statements for storing event notifications in the event log"};

processing the plurality of database events by detecting whether an executable SQL statement contains an attempt by a user to alter a set of auditing preferences existing on the database {See ROWLAND, C5:L61-67, wherein this reads over "name a local directory in an odd way to hide their work"};

forwarding the processed database events to a network accessible console {See BAPAT, C16:L40-54, wherein this reads over "each database tables stores a different type of event notification"};

recording the processed database events to a table in the database {See BAPAT, C16:L31-39, wherein this reads over "a log server 290 whose primary function is to convert event notifications into SQL insert statements for storing event notifications in the event log"}.

Art Unit: 2161

While BAPAT fails to expressly disclose a method "wherein said unauthorized activity is interfering with auditing settings," ROWLAND discloses a method wherein "[i]f a suspicious directory name is found 68, the control function is notified 55" {See ROWLAND, C6:L4-11}. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by BAPAT by combining it with the invention disclosed by ROWLAND.

One of ordinary skill in the art would have been motivated to do this modification so that suspicious or malicious activity may be detected and prevented accordingly.

17. As per dependent claim 95, BAPAT, in combination with ROWLAND, discloses:

The computer readable medium having code to perform the computer implemented method for protecting the database of Claim 89 wherein the step of analyzing further comprises the step of:

installing a listener agent as a first lightweight module, the listener agent for receiving a plurality of database events {See BAPAT, C16:L62-66, wherein this reads over "[t]he log server 290 is preferably a software entity or process that runs on the same computer or computer node as the MIS"};

establishing a communication link between the listener agent and the database {See BAPAT, C16:L55-61, wherein this reads over "only the log server 290 (besides the system administrator) has write access to the event log tables"};

using the listener agent to process the plurality of database events {See BAPAT, C16:L31-39, wherein this reads over "a log server 290 whose primary function is to convert event notifications into SQL insert statements for storing event notifications in the event log"};

processing the plurality of database events by detecting whether an executable SQL statement contains an attempt by a user to perform a write operation to a set of audit records existing in a log file before permission to write to the log file is granted {See ROWLAND, C6:L4-11, wherein this reads over "[t]he system checks to determine if the system audit records have been altered or are missing"};

forwarding the processed database events to a network accessible console {See BAPAT, C16:L40-54, wherein this reads over "each database tables stores a different type of event notification"};

recording the processed database events to a table in the database {See BAPAT, C16:L31-39, wherein this reads over "a log server 290 whose primary function is to convert event notifications into SQL insert statements for storing event notifications in the event log"}.

While BAPAT fails to expressly disclose a method "wherein said unauthorized activity is interfering with audit records," ROWLAND discloses a method wherein "[t]he system checks to determined if the system audit records have been altered or are missing" {See ROWLAND, C6:L4-11}. Therefore, it would

Art Unit: 2161

have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by BAPAT by combining it with the invention disclosed by ROWLAND.

One of ordinary skill in the art would have been motivated to do this modification so that suspicious or malicious activity may be detected and prevented accordingly.

18. As per dependent claim 96, BAPAT, in combination with ROWLAND, discloses:

The computer readable medium having code to perform the computer implemented method for protecting the database of Claim 89 wherein the step of analyzing further comprises the step of:

installing a listener agent as a first lightweight module, the listener agent for receiving a plurality of database events {See BAPAT, C16:L62-66, wherein this reads over "[t]he log server 290 is preferably a software entity or process that runs on the same computer or computer node as the MIS"};

establishing a communication link between the listener agent and the database {See BAPAT, C16:L55-61, wherein this reads over "only the log server 290 (besides the system administrator) has write access to the event log tables"};

using the listener agent to process the plurality of database events {See BAPAT, C16:L31-39, wherein this reads over "a log server 290 whose primary function is to convert event notifications into SQL insert statements for storing event notifications in the event log"};

processing the plurality of database events by detecting whether an executable SQL statement contains an attempt by a user to obtain administrator access by changing a configuration file in the database {See ROWLAND, C5:L53-56, wherein this reads over "[t]he system examines the rhost file and other system authentication files to determine if dangerous security modifications to the host file have occurred"};

forwarding the processed database events to a network accessible console {See BAPAT, C16:L40-54, wherein this reads over "each database tables stores a different type of event notification"};

recording the processed database events to a table in the database {See BAPAT, C16:L31-39, wherein this reads over "a log server 290 whose primary function is to convert event notifications into SQL insert statements for storing event notifications in the event log"}.

While BAPAT fails to expressly disclose a method "wherein said unauthorized activity is modifying security settings," ROWLAND discloses a method wherein "[t]he system examines the rhost file and other system authentication files to determine if dangerous security modifications to the host file have occurred" {See ROWLAND, C5:L53-56}. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by BAPAT by combining it with the invention disclosed by ROWLAND.

Art Unit: 2161

One of ordinary skill in the art would have been motivated to do this modification so that suspicious or malicious activity may be detected and prevented accordingly.

19. As per dependent claim 97, BAPAT, in combination with ROWLAND, discloses:

The computer readable medium having code to perform the computer implemented method for protecting the database of Claim 89 wherein the step of analyzing further comprises the step of:

installing a listener agent as a first lightweight module, the listener agent for receiving a plurality of database events {See BAPAT, C16:L62-66, wherein this reads over "[t]he log server 290 is preferably a software entity or process that runs on the same computer or computer node as the MIS"};

establishing a communication link between the listener agent and the database {See BAPAT, C16:L55-61, wherein this reads over "only the log server 290 (besides the system administrator) has write access to the event log tables"};

using the listener agent to process the plurality of database events {See BAPAT, C16:L31-39, wherein this reads over "a log server 290 whose primary function is to convert event notifications into SQL insert statements for storing event notifications in the event log"};

processing the plurality of database events by detecting whether an executable SQL statement contains an attempt by a user to use a port scanner {See ROWLAND, C6:L36-67, wherein this reads over "[t]he port scan detector of the present invention alerts administrators that a person is actively looking for services on their host"};

forwarding the processed database events to a network accessible console {See BAPAT, C16:L40-54, wherein this reads over "each database tables stores a different type of event notification"};

recording the processed database events to a table in the database {See BAPAT, C16:L31-39, wherein this reads over "a log server 290 whose primary function is to convert event notifications into SQL insert statements for storing event notifications in the event log"}.

While BAPAT fails to expressly disclose a method "wherein said unauthorized activity is a use of an unauthorized tool to attempt to access said database application," ROWLAND discloses a method wherein "[t]he port scan detector of the present invention alerts administrators that a person is actively looking for services on their host" using "a program that may either connect to all ports on the remote machine or deliberately pick one or more ports to search" {See ROWLAND, C6:36-67}. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by BAPAT by combining it with the invention disclosed by ROWLAND.

Art Unit: 2161

One of ordinary skill in the art would have been motivated to do this modification so that suspicious or malicious activity may be detected and prevented accordingly.

Response to Arguments

20. Applicant's arguments filed 3 July 2007 have been fully considered but they are not persuasive.

a. Claim Rejections under 35 U.S.C. 102

Applicant asserts the argument that "claim 90 does not require a user to request information from 'tables', nor does the Applicant's claimed invention require a 'SQL engine' to reject said request." See Amendment, page 22. The Examiner respectfully disagrees in that it would be inherent to the claimed invention that a SQL engine be present wherein a SQL statement is executed "when the discrete database event is compliant with the predefined set of rules." Furthermore, while BAPAT indeed does disclose the use of a SQL engine in rejecting a request, said disclosure would properly read upon the claimed invention as a functionally equivalent method of analyzing SQL statements for compliance with a pre-defined set of detection rules.

Accordingly, the rejections under 35 U.S.C. 102 are sustained.

b. Claim Rejections under 35 U.S.C. 103

Applicant's request for an affidavit or declaration setting forth specific factual statements is moot as Applicant has cancelled claim 25.

Conclusion

21. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date

Art Unit: 2161

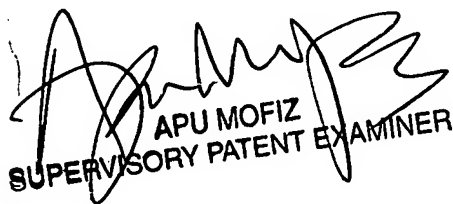
of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

22. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul Kim whose telephone number is (571) 272-2737. The examiner can normally be reached on M-F, 9am - 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Apu Mofiz can be reached on (571) 272-4080. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Paul Kim
Patent Examiner, Art Unit 2161
TECH Center 2100


APU MOFIZ
SUPERVISORY PATENT EXAMINER